

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日

Date of Application:

2000年11月22日

出願番号

Application Number:

特願2000-355968

願人

Applicant(s):

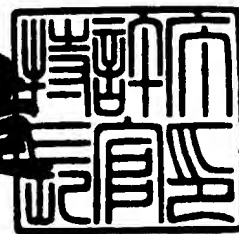
ミノルタ株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 1月26日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2001-3000722

【書類名】 特許願

【整理番号】 174604

【提出日】 平成12年11月22日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 9/00

【発明者】

【住所又は居所】 大阪府大阪市中央区安土町二丁目3番13号大阪国際ビ
ル ミノルタ株式会社内

【氏名】 正木 賢治

【特許出願人】

【識別番号】 000006079

【住所又は居所】 大阪府大阪市中央区安土町二丁目3番13号大阪国際ビ
ル

【氏名又は名称】 ミノルタ株式会社

【代理人】

【識別番号】 100062144

【弁理士】

【氏名又は名称】 青山 葆

【選任した代理人】

【識別番号】 100086405

【弁理士】

【氏名又は名称】 河宮 治

【先の出願に基づく優先権主張】

【出願番号】 特願2000- 73

【出願日】 平成12年 1月 4日

【手数料の表示】

【予納台帳番号】 013262

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9808001

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 出力システム及びそれに用いる出力方法並びに出力システムにおいて実行されるプログラムを記録した記録媒体

【特許請求の範囲】

【請求項1】 データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて、

上記データ処理装置に、上記出力装置を制御し得るドライバソフトウェアが組み込まれており、

上記データ処理装置から出力装置へのデータ送信に際し、上記ドライバソフトウェアを経由する出力要求であるか否かを判断する判断手段と、上記ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止する禁止手段とを有していることを特徴とする出力システム。

【請求項2】 データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて、

上記データ処理装置に、上記出力装置を制御し得るドライバソフトウェアが組み込まれており、

上記データ処理装置側で、上記ドライバソフトウェアを経由するデータを暗号化する暗号化手段と、

上記出力装置側で、上記暗号化手段により暗号化されたデータを解読する解読手段とを有していることを特徴とする出力システム。

【請求項3】 データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて、

上記データ処理装置に、上記出力装置を制御し得るドライバソフトウェアが組み込まれており、

上記データ処理装置から出力装置へのデータ出力要求に対して、上記出力装置へデータを出力するための設定値とは異なる設定値を設定することにより、上記出力装置へのデータ出力を禁止する禁止手段を有していることを特徴とする出力システム。

【請求項4】 上記設定値は、所定のレジスタに格納される値であることを

特徴とする請求項 3 記載の出力システム。

【請求項 5】 データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムに用いる出力方法において、

上記データ処理装置から出力装置へのデータ送信に際し、該データ処理装置に組み込まれた、上記出力装置を制御し得るドライバソフトウェアを経由する出力要求であるか否かを判断した上で、該ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止することを特徴とする出力方法。

【請求項 6】 データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムに用いる出力方法において、

上記データ処理装置側で、該データ処理装置に組み込まれたドライバソフトウェアを経由するデータを暗号化し、

上記出力装置側で、暗号化されたデータを解読するステップを有していることを特徴とする出力方法。

【請求項 7】 データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて実行されるプログラムを記録した記録媒体であって、該プログラムが、

上記データ処理装置から出力装置へのデータ送信に際し、該データ処理装置に組み込まれた、上記出力装置を制御し得るドライバソフトウェアを経由する出力要求であるか否かを判断するステップと、該ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止するステップとを有していることを特徴とするコンピュータ読取り可能な記録媒体。

【請求項 8】 データを所定の形式で出力する出力装置に対してデータを出力するデータ処理装置において実行されるプログラムを記録した記録媒体であって、該プログラムが、

アプリケーションプログラムから出力される出力データに対して所定の暗号化処理を行なうステップと、

上記暗号化ステップにより暗号化された出力データを上記出力装置に対して出

力するステップとを有していることを特徴とするコンピュータ読取り可能な記録媒体。

【請求項 9】 上記暗号化処理ステップは、アプリケーションプログラムから出力される出力データに対して、所定のパスワードを設定するステップであることを特徴とする請求項 8 記載のコンピュータ読取り可能な記録媒体。

【請求項 10】 データを所定の形式で出力する出力装置に対してデータを出力するデータ処理装置に、上記出力装置を使用可能にするためのドライバソフトウェアをインストールするインストールプログラムを記録した記録媒体であって、該インストールプログラムが、

上記データ処理装置にドライバソフトウェアをインストールするステップと、

上記ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止するプログラムをインストールするステップとを有していることを特徴とするコンピュータ読取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、プリント又はコピーを出力するための出力システムに関する。

【0002】

【従来の技術】

近年、カラー複写機、カラープリンタ若しくはカラスキャナなどの性能向上及び低価格化が進むにつれ、不正なプリント又はコピー（例えば紙幣、有価証券若しくは金券のプリント又はコピー）が容易に行える環境になりつつある。

【0003】

図 11 に、従来の典型的な出力システムにおけるデータの流れを示す。この出力システムは、基本ソフトウェアであるオペレーティングシステム（以下、OS という）52 及び該 OS 52 からの制御データに基づいて動作するハードウェア 55 を含むコンピュータ 50 と、該コンピュータ 50 に接続されたプリンタ 60 とから構成される。上記コンピュータ 50 では、OS 52 により、例えば画面の表示や文書の保存などの各種の機能が提供されるようになっている。この OS 5

2は、その中核部分であるカーネルとは切り離してプリンタを制御し得るプリンタドライバソフトウェア(以下、プリンタドライバという)53を有しており、また、OS52の一部には、アプリケーションプログラム(図中のアプリケーションA及びB)の各種要求に応じて、OS52上の各種機能呼び出す仕様としてのAPI(Application Programming Interface)54が設定されている。

【0004】

一般に、汎用のOSが組み込まれたコンピュータを含む出力システムにおいて印刷が行われる場合には、アプリケーションプログラムからのプリント要求に応じて、プリンタドライバ53及びAPI54を順次呼び出し、プリンタドライバ53上でデータを作成した上で、ハードウェア55のプリンタI/O56へ送信する方法(図中、アプリケーションAからの経路)、及び、プリンタドライバ53上でデータを作成することなく、アプリケーションプログラムからAPI54を介してハードウェア55のプリンタI/O56へ直接に送信される方法(図中、アプリケーションBからの経路)の2通りの方法が実施可能である。

【0005】

【発明が解決しようとする課題】

ところで、従来、かかる出力システムにおいて、不正なプリント又はコピーを防止するには、プリンタドライバ53に不正プリント／コピー防止機能をもたせることが一般的である。しかし、前述したような出力システムでは、例えば、プリント対象であるデータをコンピュータ50側で圧縮し、プリンタ60側で伸張する処理を行なう場合など、コンピュータ50から出力されるデータを取り出して解析することにより、プリンタ60での処理内容を解読する場合には、プリンタドライバ53を迂回して、すなわち、プリンタドライバ53上でデータを作成することなく、プリンタ60へアクセスすることが可能となっており、この経路では、不正プリント／コピーを防止することができない。

【0006】

なお、現在、カラー複写機については、不正プリント／コピー防止用手段の装備が義務付けられているが、このような付加的な手段は、一般的に、ハードウェアとして実装されるため、機器のコスト増大を回避し得ない。

また、例えばLAN等の、複数台のコンピュータ及び該コンピュータに接続される複数台のプリンタから構成されるシステムにおいては、プリンタ側に不正プリント／コピー防止用装置を設置する場合、個々のプリンタが同様の不正プリント／コピー防止用装置をもつことになり、無駄が生じる。

【0007】

そこで、本発明は、上記技術的課題に鑑みてなされたもので、安価且つ安全な出力システム及びそれに用いる出力方法並びに出力システムにおいて実行されるプログラムを記録した記録媒体を提供することを目的とする。

【0008】

【課題を解決するための手段】

本願の請求項1に係る発明は、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて、上記データ処理装置に、上記出力装置を制御し得るドライバソフトウェアが組み込まれており、上記データ処理装置から出力装置へのデータ送信に際し、上記ドライバソフトウェアを経由する出力要求であるか否かを判断する判断手段と、上記ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止する禁止手段とを有していることを特徴としたものである。

【0009】

また、本願の請求項2に係る発明は、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて、上記データ処理装置に、上記出力装置を制御し得るドライバソフトウェアが組み込まれており、上記データ処理装置側で、上記ドライバソフトウェアを経由するデータを暗号化する暗号化手段と、上記出力装置側で、上記暗号化手段により暗号化されたデータを解読する解読手段とを有していることを特徴としたものである。

【0010】

更に、本願の請求項3に係る発明は、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて、上記データ処理装置に、上記出力装置を制御し得る不正プリント防止

機能を備えたドライバソフトウェアが組み込まれており、上記データ処理装置から出力装置へのデータ出力要求に対して、上記出力装置へデータを出力するための設定値とは異なる設定値を設定することにより、上記出力装置へのデータ出力を禁止する禁止手段を有していることを特徴としたものである。

【 0 0 1 1 】

また、更に、本願の請求項4に係る発明は、請求項3に係る発明において、上記設定値が、所定のレジスタに記憶される値であることを特徴としたものである。

【 0 0 1 2 】

また、更に、本願の請求項5に係る発明は、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムに用いる出力方法において、上記データ処理装置から出力装置へのデータ送信に際し、該データ処理装置に組み込まれた、上記出力装置を制御し得るドライバソフトウェアを経由する出力要求であるか否かを判断した上で、該ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止することを特徴としたものである。

【 0 0 1 3 】

また、更に、本願の請求項6に係る発明は、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムに用いる出力方法において、上記データ処理装置側で、該データ処理装置に組み込まれたドライバソフトウェアを経由するデータを暗号化し、上記出力装置側で、暗号化されたデータを解読するステップを有していることを特徴としたものである。

【 0 0 1 4 】

また、更に、本願の請求項7に係る発明は、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて実行されるプログラムを記録した記録媒体であって、該プログラムが、上記データ処理装置から出力装置へのデータ送信に際し、該データ処理装置に組み込まれた、上記出力装置を制御し得るドライバソフトウェアを経由する

出力要求であるか否かを判断するステップと、該ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止するステップとを有していることを特徴としたものである。

【0015】

また、更に、本願の請求項8に係る発明は、データを所定の形式で出力する出力装置に対してデータを出力するデータ処理装置において実行されるプログラムを記録した記録媒体であって、該プログラムが、アプリケーションプログラムから出力される出力データに対して所定の暗号化処理を行なうステップと、上記暗号化ステップにより暗号化された出力データを上記出力装置に対して出力するステップとを有していることを特徴としたものである。

【0016】

また、更に、本願の請求項9に係る発明は、請求項8に係る発明において、上記暗号化処理ステップが、アプリケーションプログラムから出力される出力データに対して、所定のパスワードを設定するステップであることを特徴としたものである。

【0017】

また、更に、本願の請求項10に係る発明は、データを所定の形式で出力する出力装置に対してデータを出力するデータ処理装置に、上記出力装置を使用可能にするためのドライバソフトウェアをインストールするインストールプログラムを記録した記録媒体であって、該インストールプログラムが、上記データ処理装置にドライバソフトウェアをインストールするステップと、上記ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止するプログラムをインストールするステップとを有していることを特徴としたものである。

【0018】

【発明の実施の形態】

以下、本発明の実施の形態について、添付図面を参照しながら説明する。

実施の形態1.

図1は、本発明の実施の形態1に係る出力システムを含むネットワークを示す

説明図である。このネットワーク 1 0 0 は、ネットワーク全体の制御、管理等および他のネットワーク構成から要求されるファイル検索などの仕事を実行するサーバコンピュータ 1 2 と、複数台のクライアントコンピュータ 1 0 と、該クライアントコンピュータ 1 0 から送信されてきたデータを印字プリントとして出力するプリンタ 2 0 とを有している。上記サーバコンピュータ 1 2 には、各種のデータを系統的に管理するデータベース 1 2 A が付属させられ、該データベース 1 2 A は、必要に応じて、各クライアントコンピュータ 1 0 からアクセスされ、データの書込み又は読出しが行われる。

【 0 0 1 9 】

各クライアントコンピュータ 1 0 は、基本ソフトウェアであるオペレーティングシステム(以下、OS という) 2 及び該 OS 2 の制御データに基づいて動作するハードウェア 5 (OS 2 及びハードウェア 5 とともに図 2 参照) を含んでおり、ネットワーク 1 0 0 がインターネット 1 9 に接続されていることから、これらクライアントコンピュータ 1 0 では、例えば電子メールや FTP (File Transfer Protocol) によるファイル転送、WWW によるホームページ閲覧、該ホームページからの各種形式データのダウンロード等のサービスが利用可能である。ここでは、クライアントコンピュータ 1 0 に組み込まれる OS 2 として、ウィンドウズ (Windows) が採用されている。なお、これに限定されることなく、例えばユニックス (UNIX) 若しくは MS-DOS 等の汎用 OS を採用してもよい。

【 0 0 2 0 】

本実施の形態に係る出力システムは、クライアントコンピュータ 1 0 からプリンタ 2 0 へデータ送信するに際して、不正なプリント又はコピーを防止すべく、不正なジョブデータについては、その送信を禁止する若しくはプリンタ 2 0 側での出力を禁止することを可能とする、クライアントコンピュータ 1 0 とそれに接続されたプリンタ 2 0 とから構成される出力システムである。以下、この出力システムについて説明する。なお、以下の説明では、クライアントコンピュータ 1 0 を単にコンピュータ 1 0 という。

【 0 0 2 1 】

図 2 は、コンピュータ 1 0 とプリンタ 2 0 とから構成される出力システムの構

成を示す説明図である。コンピュータ 10 では、OS 2 により例えば画面の表示や文書の保存などの各種の機能が提供されるようになっており、OS 2 が、その中核部分であるカーネルとは切り離して所定のハードウェアを制御し得るソフトウェア形態のデバイスドライバを複数有しており、これらデバイスドライバの 1 つとして、プリンタ 20 を制御し得るプリンタドライバ 3 がインストールされている。プリンタドライバ 3 は、一般的に、プリンタ本体販売時に同梱されている CD-ROM 15 又はフロッピーディスク 16 等の外部記録媒体より、コンピュータ 10 にインストールされる。通常、このプリンタドライバ 3 のインストールに際して、プリンタドライバ 3 のインストールをユーザの目的に応じて半自動又は自動的に行なえるようにするためのプログラムであるインストーラが用意されており、このインストーラプログラムが、CD-ROM 15 又はフロッピーディスク 16 等の外部記録媒体より、コンピュータ 10 にプリンタドライバをインストールする。

【0022】

また、OS 2 の一部には、アプリケーションプログラム(図中のアプリケーション A 及び B)のプリント要求に応じて、OS 2 上のプリント機能呼び出す仕様としての API 4 (図中では「Modified API」と表記)が設定されている。この実施の形態 1 において、API 4 は、OS 2 上に予め設定されていた API、すなわち、アプリケーションプログラムからプリンタへの直接的なアクセスを可能とする API (従来例を示す図 11 参照)が置き換えられてなるもので、詳しくは図 3 のフローチャートを参照して後述するが、この API 4 は、プリンタドライバ 3 を迂回してきたデータについて、プリンタ 20 へのデータ送信機能を無効とし、これにより、データが API 3 を介してプリンタ 20 へ直接に送られることを禁止し得る。

【0023】

API 4 は、前述したプリンタドライバ 3 のインストール時に、CD-ROM 15 又はフロッピーディスク 16 より、コンピュータ 10 にインストールされる。このインストールに際して、OS 2 上に存在していたオリジナルの API は、上書きされてディスク上に存在しなくなるか、若しくは、バックアップファイル

として別名に書き換えられる。これにより、図 2 に示す OS 2 では、アプリケーション A 及び B からのプリント要求に応じて、常時、新たにインストールされた API 4 が呼び出されるようになっている。

OS 2 として、例えばウィンドウズ (Windows) を採用する場合、API は DLL ファイルとして提供される。API 4 のインストールにより、オリジナルの DLL ファイルは、新たにインストールされる DLL ファイルに置き換えられる。

【0024】

以上の構成を備えた OS 2 では、通常、アプリケーション A 及び B からのプリント要求に応じて、まず、プリンタドライバ 3 が、アプリケーションプログラムからのプリント要求に応じて呼び出され、続いて、API 4 が呼び出される。そして、データがプリンタドライバ 3 を経由するものであるか否かを判断し、プリンタドライバ 3 を経由する場合には、プリンタドライバ 3 上でのデータ作成処理が行なわれる。その後、データは、ハードウェア 5 に組み込まれたプリンタ I/O 6 へ入力され、プリンタ 20 への送信に適した形式に変換された上で送信される。

【0025】

このプリンタドライバ 3 では、従来知られるように、プリント対象であるデータを作成するに際して、不正なプリントの防止を可能とし、不正なジョブデータを受けた場合、そのデータについては、プリンタ 20 へのアクセスを拒否することができる。このように、プリンタドライバ 3 を経由した場合には、不正なデータがプリンタ 20 へのアクセスを拒否されるようになっており、不正プリントの防止が実現される。

【0026】

また、一方、データがプリンタドライバ 3 を経由しない場合、すなわち、データがプリンタドライバ 3 を迂回する場合、この実施の形態 1 では、OS 2 において、API 4 のファンクションコール（以下、API コールという）がトラップされて独自のルーチンに置き換えられることで、プリンタへのデータ送信機能が無効にされ、これにより、一切のデータが API 4 を介してプリンタ 20 へ直接

に送られることが禁止される。その結果、不正なデータは、プリンタ 8 へのアクセスを拒否され、不正プリントの防止が実現される。

【 0 0 2 7 】

図 3 は、出力システムにおける不正プリント防止動作についてのフローチャートである。まず、# 1 1 では、アプリケーションプログラムからのプリント要求に応じて、プリンタドライバ 3 を呼び出し、続いて、# 1 2 では、API 4 を呼び出す。# 1 3 では、プリント要求をあらわす API コールをトラップする。そして、# 1 4 では、API コールに基づき、プリンタドライバ 3 の経由が要求されているか否かを判断する。その結果、プリンタドライバ 4 の経由が要求されない場合には、# 1 5 へ進み、プリンタ 2 0 への直接アクセスを禁止して、処理を終了する。他方、プリンタドライバ 4 の経由が要求される場合、# 1 6 へ進む。

【 0 0 2 8 】

1 6 では、プリンタドライバ 3 に予め組みこまれている不正プリント防止機能呼び出す。続いて、# 1 7 では、不正プリントであるか否か、すなわち、プリント対象であるデータが不正なデータであるか否かを判断する。その結果、不正プリントである場合には、# 1 8 へ進み、プリンタ 2 0 へのアクセスを拒否して、処理を終了する。他方、不正なプリントではない場合には、# 1 9 へ進み、プリンタ 2 0 へアクセスする。その後、# 2 0 では、プリンタ 2 0 にて、データに基づき印刷を行ない、プリントを出力する。

【 0 0 2 9 】

このようにして、上記出力システムでは、プリンタドライバ 3 を経由する場合および迂回する場合共に、不正なプリントを防止することができる。かかる不正プリント防止動作は、コンピュータ 1 0 に組み込まれた OS 2 のプログラムに基づいて実行されるものであり、この実施の形態 1 では、該プログラムが、コンピュータ 1 0 内のハードディスクにインストールされており、メモリ上に呼び出されて実行される。なお、これに限定されることなく、このようなプログラムは、例えばフロッピーディスク、CD-ROM 等の外部記録媒体にファイル形式で保存され、そこから呼び出すようにしてもよい。

【 0 0 3 0 】

以上のように、この実施の形態 1 では、ハードウェア面での追加投資なしに、ソフトウェア面における補充を行うのみにより、安価で且つ信頼性の高い不正プリントの防止が可能な出力システムを実現することができる。また、この場合には、プリンタドライバ 4 に不正プリントの防止技術が搭載されるため、ドライバ自体のアップデートが容易であり、例えば新紙幣等の新規の不正プリント対象への対応を簡単に実施することができる。

【 0 0 3 1 】

なお、この実施の形態 1 では、プリンタドライバ 3、そのインストーラ、API 4 が、CD-ROM 1 5 又はフロッピーディスク 1 6 等の外部記録媒体より、コンピュータ 1 0 にインストールされるが、これに限定されることなく、コンピュータ 1 0 に接続された LAN やネットワークを介して、他のコンピュータからドライバソフトウェアをダウンロード及びインストールするようにしてもよい。

【 0 0 3 2 】

また、図 4 には、インストーラによるプリンタドライバ 3 及び API 4 のインストール動作についてのフローチャートを示す。このインストール動作では、コンピュータ 1 0 にプリンタドライバ 3 をインストールし（# 2 1）、続いて、API 4 をインストールする（# 2 2）。# 2 1 及び # 2 2 のステップは、これに限定されることなく、順序を入れ替えられても若しくは並行して行なわれてもよい。

【 0 0 3 3 】

実施の形態 2.

図 5 は、本発明の実施の形態 2 に係る出力システムの構成を示す説明図である。この出力システムは、前述した実施の形態 1 における場合と同様に、基本ソフトウェアである OS 3 2 及びその制御データに基づいて動作するハードウェア 3 5 を含むコンピュータ 3 0 と、該コンピュータ 3 1 に接続されたプリンタ 4 0 とから構成される。OS 3 2 は、ソフトウェア形態のデバイスドライバの 1 つとして、プリンタ 4 0 を制御し得るプリンタドライバ 3 3 を有している。また、OS 3 2 の一部には、アプリケーションプログラム(図中のアプリケーション A 及び B)のプリント要求に応じて OS 3 2 上のプリント機能呼び出す仕様としての

A P I 3 4 が設定されている。

【0034】

プリンタドライバ33は、プリント対象であるデータを作成するに際して、不正なプリントの防止を可能とし、不正なデータを受けた場合、そのデータについては、プリンタ40へのアクセスを拒否することができる。更に、この実施の形態2では、プリンタドライバ33は、正常プリントを行なう場合、すなわち、そのプリント出力が許可される正常データを受けた場合に、データの先頭にある10バイト分のデータを反転させる暗号化機能を有している。

かかるプリンタドライバ33を経由したデータ若しくは迂回したデータは、ハードウェア35に組み込まれたプリンタI/O36へ入力され、プリンタ40への送信に適した形式に変換された上で、プリンタ40へ送信される。

【0035】

この実施の形態2では、プリンタドライバ33におけるデータ反転の暗号化機能に対応して、プリンタ40に組み込まれた制御部41が、コンピュータ30より送られてきたデータの先頭にある10バイト分のデータを反転させる復号化機能（データ反転機能）を有しており、プリンタ40は、この機能によるデータ反転後に、正常なデータについて出力を続行し、異常なデータについては出力を中止する動作を行う。ここで、「正常なデータ」とは、コンピュータ30側で暗号化されたデータが、プリンタ40側で再度反転されて元の形に戻ったデータをあらわし、他方、「異常なデータ」とは、プリンタドライバ33を迂回して送信されてきたデータが、プリンタ40側で反転されてなるデータをあらわす。

【0036】

これにより、この実施の形態2に係る出力システムでは、不正なデータについて、それがプリンタドライバ33を経由する場合、その不正プリント防止機能により、出力が防止され、他方、それがプリンタドライバ33を迂回する場合には、プリンタ40の制御部41において設定された復号化機能を用いて、先頭にある10バイト分のデータが反転させられたデータが異常データとみなすことにより、不正なプリントが防止される。

【0037】

図6は、この出力システムにおける不正プリント防止動作についてのフローチャートである。まず、#31では、アプリケーションプログラムからのプリント要求に応じて、プリンタドライバ33を呼び出し、続いて、#32では、API34を呼び出す。#33では、プリント要求をあらわすAPIコールをトラップする。そして、#34では、APIコールに基づき、プリンタドライバ33の経路が要求されているか否かを判断する。その結果、プリンタドライバ4の経路が要求されない場合には、#35へ進み、他方、プリンタドライバ4の経路が要求される場合、#38へ進む。

【0038】

#35では、プリンタ40へ直接にアクセスする。続いて、#36では、プリンタ40にて、データの先頭を10バイト反転させる。#37では、データが異常データとみなされることから出力を中止し、処理を終了する。

【0039】

#38では、プリンタドライバ33に予め設定されている不正プリント防止機能呼び出す。次に、#39では、不正プリントであるか否か、すなわち、プリント対象であるデータが不正なデータであるか否かを判断する。その結果、不正プリントである場合には、#40へ進み、プリンタ40へのアクセスを拒否して、処理を終了する。他方、不正なプリントではない場合には、#41へ進み、データの先頭を10バイト反転させ、#42では、プリンタ40へアクセスする。

【0040】

続いて、#43では、プリンタ40にて、データの先頭を10バイト反転させる。これにより、プリンタドライバ33上でその先頭10バイトが反転させられた反転させられたデータが、元の正常なデータに戻る。そして、#44では、データに基づき印刷を行ない、プリントを出力する。

このようにして、上記出力システムは、プリンタドライバ33を経由する場合および迂回する場合共に、不正なプリントを防止することができる。

【0041】

なお、前述した実施の形態2では、このような不正プリント防止機能を実現する手段としてのデータ暗号化手段が、プリンタドライバ33を経由するデータの

先頭 10 バイトを反転することによるものであったが、これに限定されることなく、かかる暗号化としては、例えばプリンタドライバ 33 を経由するデータに、パスワードを付すようにしてもよい。この場合には、データ解読を行なうべく、プリンタ 40 側に、上記パスワードを認識しデータを識別するプログラムを設ける必要がある。

【 0 0 4 2 】

以上のように、この実施の形態 2 では、ハードウェア面での追加投資なしに、ソフトウェア面における補充を行うのみにより、信頼性の高い不正プリントの防止が可能で、安価なシステムを実現することができる。また、この場合には、プリンタドライバ 33 に不正プリントの防止技術が搭載されるため、ドライバ自体のアップデートが容易であり、例えば新紙幣等の新規の不正プリント対象への対応を比較的簡単に実施することができる。

また、この実施の形態 2 では、プリンタ 40 のファームウェアに上記復号化プログラムを組み込むことにより、不正プリントの防止を実現するため、コストの増大が回避されるとともに、比較的高い安全性が確保される。

【 0 0 4 3 】

実施の形態 3.

図 7 ～ 10 を参照して、コンピュータに組み込まれる OS として、MS-DOS を採用した場合について説明する。図 7 は、MS-DOS システムにおけるプリント出力時のデータの流れを概略的に示す説明図である。この MS-DOS システムでは、アプリケーションプログラム（図中の「アプリケーション」）からのプリント要求に応じて発せられたプリントの命令に対し、所定のレジスタ（AH, AL, DX レジスタ）に設定する内容として、通常プリント時に設定される値とは異なる値が設定されるように、システムを変更することにより、実質的には異なるレジスタを使用することになる。これによって、プリンタへのデータ送信を禁止して、通常のプリント動作を一切禁止することができる。

【 0 0 4 4 】

図 8 を参照して MS-DOS システムにて一般的に行なわれるデータ処理について説明する。MS-DOS システムでは、システム起動時に BIOS 割込みテ

ーブルがセットされる。アプリケーションからのプリント要求に応じ、プリント対象とされるデータを、BIOS割込み呼出しの形でプリンタへ送信する。このとき、アプリケーションが文字Aをプリントする場合に、AHレジスタに0をセットし（＃51）、文字Aに相当するデータ65をALレジスタに格納し（＃52）、DXレジスタに、出力先のプリンタ番号を指定して（＃53）、割込み命令としてのINT17命令を発する。

【0045】

INT17命令を受けたCPUは、17番に相当するアドレス（例えば「0000:005c」のアドレスから始まる4バイトに格納されているデータ）を割込みテーブルから取得する（＃54）。その後、CPUは、スタックフレームを作成して該フレーム内にレジスタを退避させたのち（＃55）、そのアドレスにジャンプして、割込みを行う（＃56）。ジャンプした場所が、本来のプリンタコントロールを行なう場所であることにより、データがプリンタへ送信された後に、リターン命令が発せられると、制御又はアプリケーションに戻る。

【0046】

図9は、本発明の実施の形態3に係るトラップ処理についてのフローチャートである。システム起動時に、自動起動されるトラッププログラムにて、BIOS割込みテーブルの「0000:005c」のアドレスから始まる4バイトの内容を、トラッププログラム内にコピーする（＃61）。続いて、トラッププログラム内の擬似プリントルーチンのアドレスを「0000:005c」から始まる4バイトにコピーし（＃62）、プログラムをメモリ上に残したまま終了する。

【0047】

次に、図10は、擬似プリントルーチンの動作についてのフローチャートである。擬似プリントルーチンでは、CHレジスタの内容をAHレジスタにコピーし（＃71）、CLレジスタの内容をALレジスタにコピーし（＃72）、また、BXレジスタの内容をDXレジスタにコピーする（＃73）。そして、プリントルーチンアドレスを読み込み（＃74）、トラッププログラム内にコピーした本体のプリントルーチンのアドレスにジャンプする（＃75）。これにより、アプリケーションから見れば、プリントの命令が、AH、AL、DXレジスタを使う

ものから、CH、CL、BXレジスタを用いるものに変更されることになり、通常のプリント動作が一切行なえなくなる。

更に、この擬似プリントルーチンは、プリンタコントロールICのポートを監視しており、データを送信していないにもかかわらず、ビジー信号が生じる場合には、異常対策として、プリンタIC初期化命令を送る。

【 0 0 4 8 】

このようにして、本プリンタドライバは、最初からCH、CL、BXレジスタを使用するものであるため、本プリンタドライバを使うアプリケーションのみについて印刷を行なうことが可能となる。また、BIOSを介さずに、データをプリンタコントロールICへ直接に送信した場合にも、ICがリセットされるため、不正な使用が防止される。

【 0 0 4 9 】

なお、本発明は、例示された実施の形態に限定されるものでなく、本発明の要旨を逸脱しない範囲において、種々の改良及び設計上の変更が可能であることは言うまでもない。

【 0 0 5 0 】

【発明の効果】

本願の請求項1に係る発明によれば、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて、上記データ処理装置に、上記出力装置を制御し得るドライバソフトウェアが組み込まれており、上記データ処理装置から出力装置へのデータ送信に際し、上記ドライバソフトウェアを経由する出力要求であるか否かを判断する判断手段と、上記ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止する禁止手段とを有しているため、信頼性の高い不正プリントの防止が可能で、安全な出力システムを実現することができる。また、かかる不正プリントの防止技術が、ソフトウェア面の補充のみで実現されるため、不正プリント防止技術としてハードウェアが装備される場合と比較して、コスト増大を著しく抑制することができる。

【 0 0 5 1 】

また、本願の請求項2に係る発明によれば、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて、上記データ処理装置に、上記出力装置を制御し得るドライバソフトウェアが組み込まれており、上記データ処理装置側で、上記ドライバソフトウェアを経由するデータを暗号化する暗号化手段と、上記出力装置側で、上記暗号化手段により暗号化されたデータを解読する解読手段とを有しているため、信頼性の高い不正プリントの防止が可能で、安全な出力システムを実現することができる。また、かかる不正プリントの防止技術が、ソフトウェア面の補充のみで実現されるため、不正プリント防止技術としてハードウェアが装備される場合と比較して、コスト増大を著しく抑制することができる。更に、この場合には、ドライバ自体のアップデートが容易であり、例えば新紙幣等の新規の不正プリント対象への対応を簡単に実施することができる。

【 0 0 5 2 】

更に、本願の請求項3に係る発明によれば、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて、上記データ処理装置に、上記出力装置を制御し得る不正プリント防止機能を備えたドライバソフトウェアが組み込まれており、上記データ処理装置から出力装置へのデータ出力要求に対して、上記出力装置へデータを出力するための設定値とは異なる設定値を設定することにより、上記出力装置へのデータ出力を禁止する禁止手段を有しているため、信頼性の高い不正プリントの防止が可能で、安全な出力システムを実現することができる。また、かかる不正プリントの防止技術が、ソフトウェア面の補充のみで実現されるため、不正プリント防止技術としてハードウェアが装備される場合と比較して、コスト増大を著しく抑制することができる。更に、この場合には、ドライバ自体のアップデートが容易であり、例えば新紙幣等の新規の不正プリント対象への対応を簡単に実施することができる。

【 0 0 5 3 】

また、更に、本願の請求項4に係る発明は、上記設定値が、所定のレジスタに格納される値であるため、信頼性の高い不正プリントの防止が可能で、安全な出

カシステムを実現することができる。

【 0 0 5 4 】

また、更に、本願の請求項 5 に係る発明によれば、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムに用いる出力方法において、上記データ処理装置から出力装置へのデータ送信に際し、該データ処理装置に組み込まれた、上記出力装置を制御し得るドライバソフトウェアを経由する出力要求であるか否かを判断した上で、該ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止するため、信頼性の高い不正プリントの防止が可能で、安全な出力システムを実現することができる。また、かかる不正プリントの防止技術が、ソフトウェア面の補充のみで実現されるため、不正プリント防止技術としてハードウェアが装備される場合と比較して、コスト増大を著しく抑制することができる。

【 0 0 5 5 】

また、更に、本願の請求項 6 に係る発明によれば、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムに用いる出力方法において、上記データ処理装置側で、該データ処理装置に組み込まれたドライバソフトウェアを経由するデータを暗号化し、上記出力装置側で、暗号化されたデータを解読するステップを有しているため、信頼性の高い不正プリントの防止が可能で、安全な出力システムを実現することができる。また、かかる不正プリントの防止技術が、ソフトウェア面の補充のみで実現されるため、不正プリント防止技術としてハードウェアが装備される場合と比較して、コスト増大を著しく抑制することができる。更に、この場合には、ドライバ自体のアップデートが容易であり、例えば新紙幣等の新規の不正プリント対象への対応を簡単に実施することができる。

【 0 0 5 6 】

また、更に、本願の請求項 7 に係る発明によれば、データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて実行されるプログラムを記録した記録媒体であって、該プログラムが、上記データ処理装置から出力装置へのデータ送信に際し、該データ

処理装置に組み込まれた、上記出力装置を制御し得るドライバソフトウェアを経由する出力要求であるか否かを判断するステップと、該ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止するステップとを有しているため、信頼性の高い不正プリントの防止が可能で、安全な出力システムを実現することができる。また、かかる不正プリントの防止技術が、ソフトウェア面の補充のみで実現されるため、不正プリント防止技術としてハードウェアが装備される場合と比較して、コスト増大を著しく抑制することができる。更に、この場合には、ドライバ自体のアップデートが容易であり、例えば新紙幣等の新規の不正プリント対象への対応を簡単に実施することができる。

【 0 0 5 7 】

また、更に、本願の請求項 8 に係る発明によれば、データを所定の形式で出力する出力装置に対してデータを出力するデータ処理装置において実行されるプログラムを記録した記録媒体であって、該プログラムが、アプリケーションプログラムから出力される出力データに対して所定の暗号化処理を行なうステップと、上記暗号化ステップにより暗号化された出力データを上記出力装置に対して出力するステップとを有しているため、信頼性の高い不正プリントの防止が可能で、安全な出力システムを実現することができる。また、かかる不正プリントの防止技術が、ソフトウェア面の補充のみで実現されるため、不正プリント防止技術としてハードウェアが装備される場合と比較して、コスト増大を著しく抑制することができる。更に、この場合には、ドライバ自体のアップデートが容易であり、例えば新紙幣等の新規の不正プリント対象への対応を簡単に実施することができる。

【 0 0 5 8 】

また、更に、本願の請求項 9 に係る発明によれば、上記暗号化処理ステップが、アプリケーションプログラムから出力される出力データに対して、所定のパスワードを設定するステップであり、信頼性の高い不正プリントの防止が可能で、安全な出力システムを実現することができる。

【 0 0 5 9 】

また、更に、本願の請求項 1 0 に係る発明によれば、データを所定の形式で出

力する出力装置に対してデータを出力するデータ処理装置に、上記出力装置を使用可能にするためのドライバソフトウェアをインストールするインストールプログラムを記録した記録媒体であって、該インストールプログラムが、上記データ処理装置にドライバソフトウェアをインストールするステップと、上記ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止するプログラムをインストールするステップとを有しているため、信頼性の高い不正プリントの防止が可能で、安全な出力システムを実現することができる。また、かかる不正プリントの防止技術が、ソフトウェア面の補充のみで実現されるため、不正プリント防止技術としてハードウェアが装備される場合と比較して、コスト増大を著しく抑制することができる。更に、この場合には、ドライバ自体のアップデートが容易であり、例えば新紙幣等の新規の不正プリント対象への対応を簡単に実施することができる。

【図面の簡単な説明】

【図 1】 本発明の実施の形態 1 に係る出力システムが組み込まれたネットワークシステムを示す図である。

【図 2】 上記出力システムの構成を示す説明図である。

【図 3】 上記出力システムによる不正プリント防止動作のフローチャートである。

【図 4】 インストーラによるプリンタドライバ及び API のインストール動作のフローチャートである。

【図 5】 本発明の実施の形態 2 に係る出力システムの構成を示す説明図である。

【図 6】 上記実施の形態 2 に係る出力システムによる不正プリント防止動作のフローチャートである。

【図 7】 本発明の実施の形態 3 に係る MS-DOS システムを採用した場合におけるデータの流れを概略的に示す説明図である。

【図 8】 MS-DOS システムにて一般的に行なわれるデータ処理のフローチャートである。

【図 9】 上記実施の形態 3 に係るトラップ処理のフローチャートである。

【図 1 0】 上記実施の形態 3 に係る疑似プリントルーチンである。

【図 1 1】 従来の出力システムの構成の一例を示す説明図である。

【符号の説明】

1 0, 3 0 … コンピュータ

2, 3 2 … オペレーティングシステム

3, 3 3 … プリンタドライバ

4, 3 4 … A P I

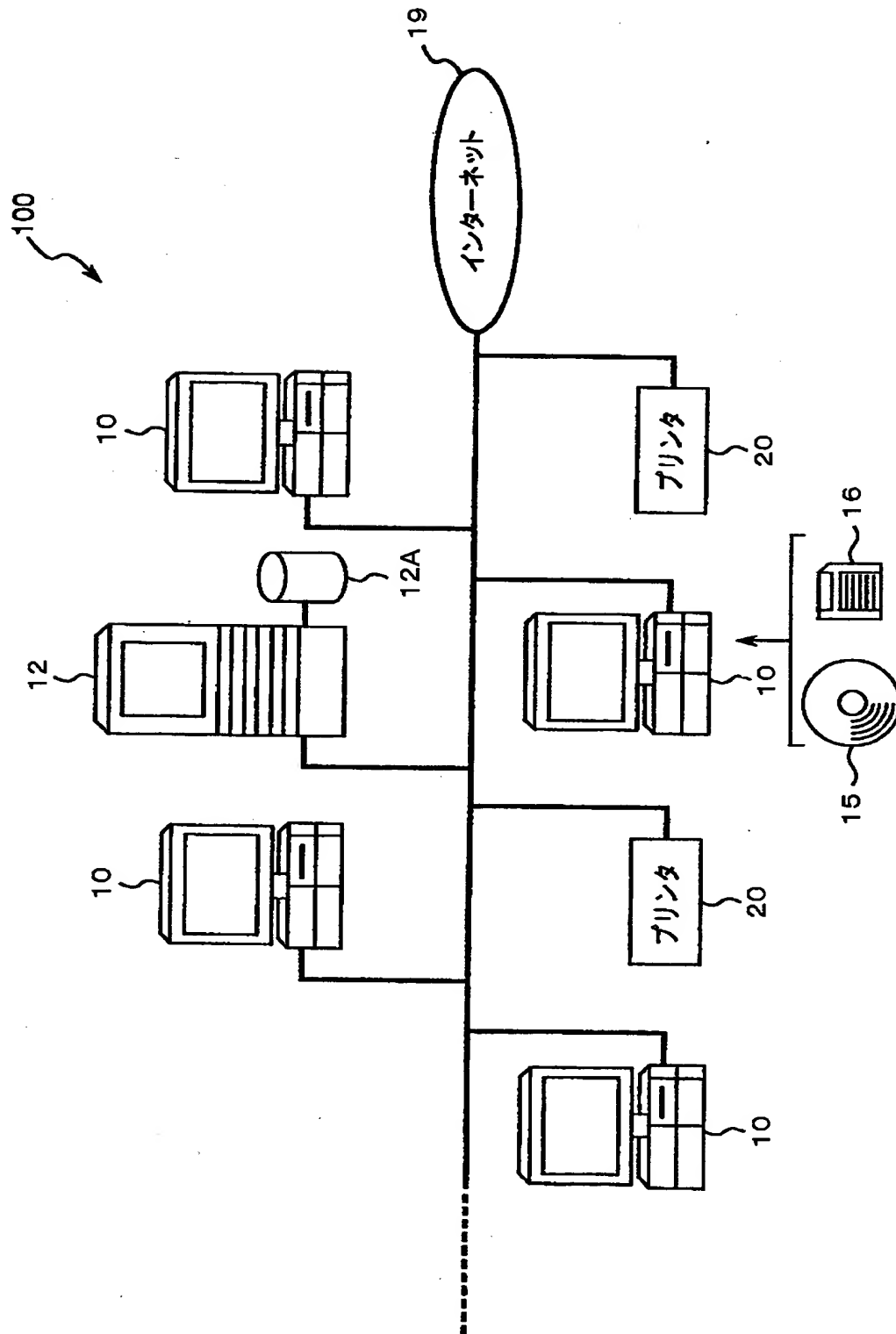
2 0, 4 0 … プリンタ

4 1 … プリンタ制御部

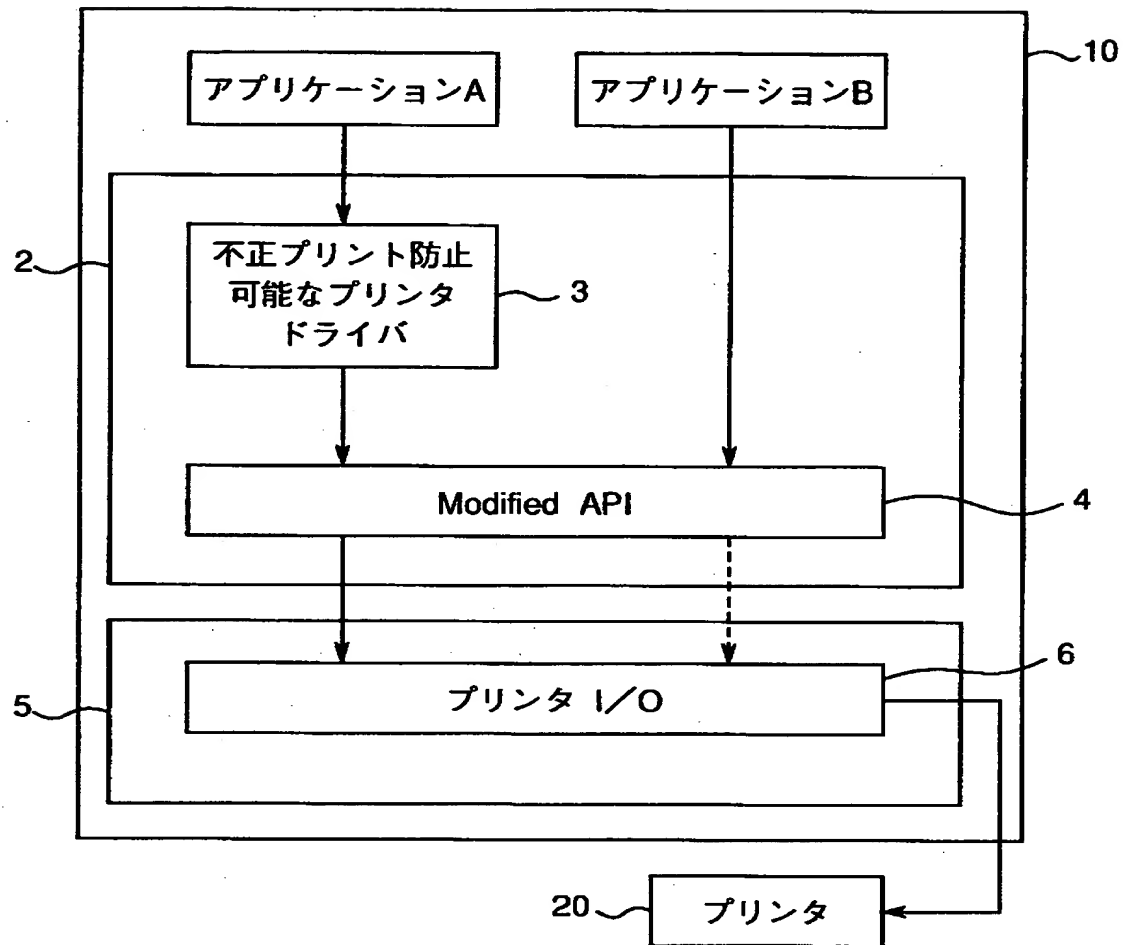
1 0 0 … ネットワーク

【書類名】 図面

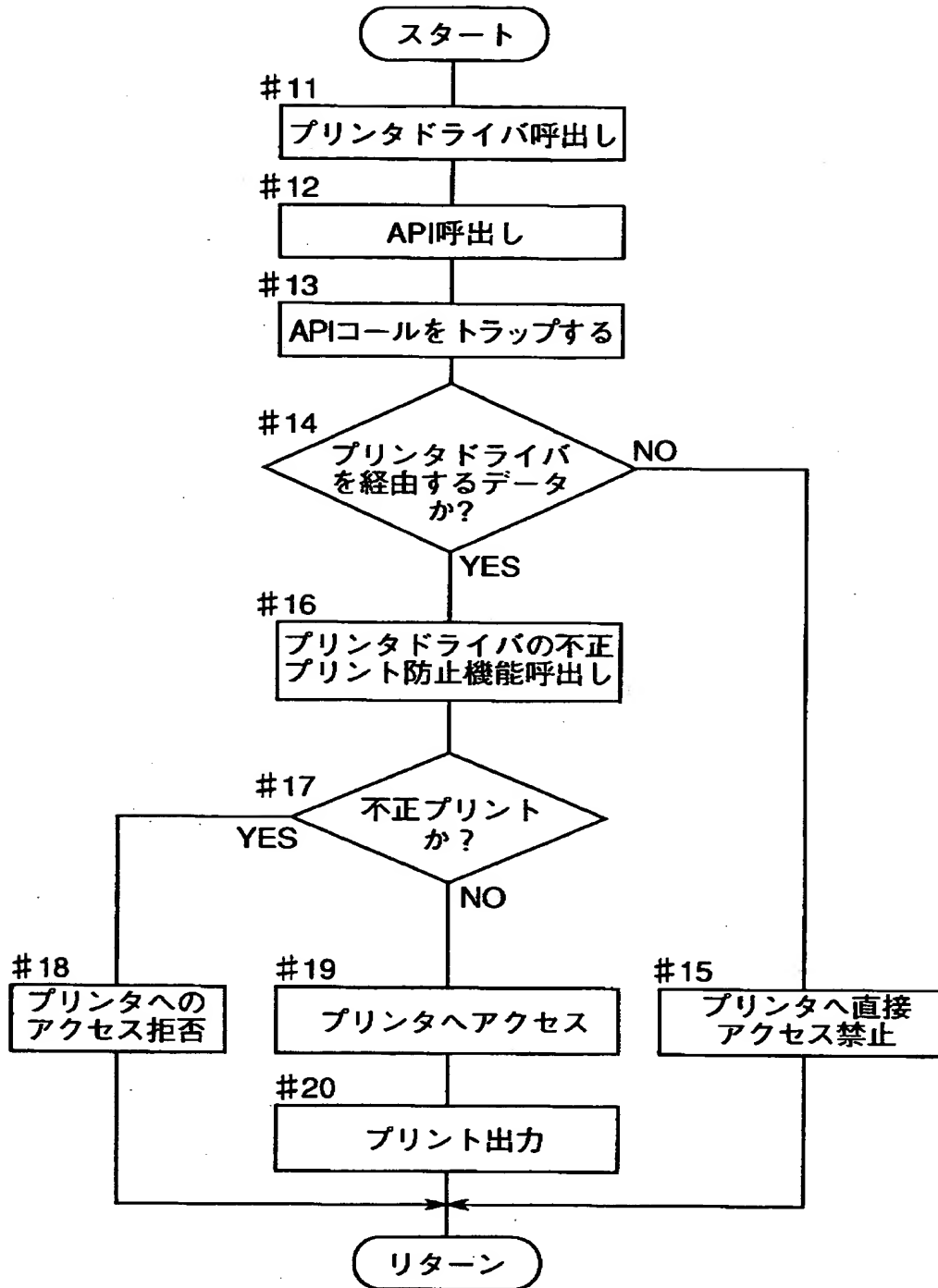
【図 1】



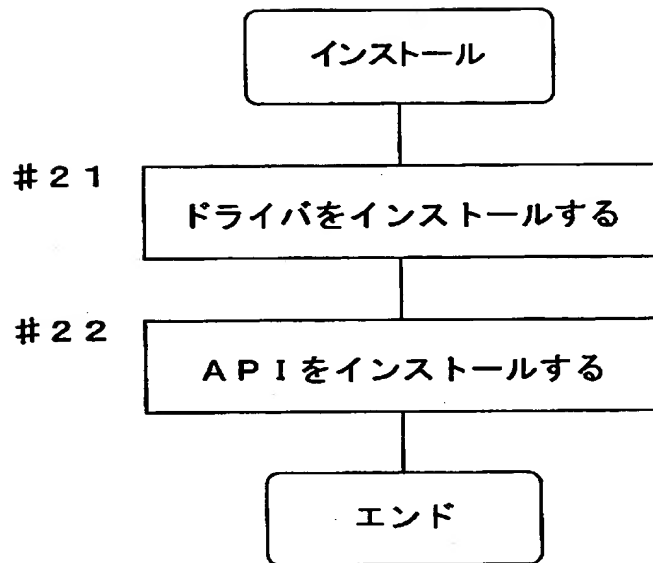
【図 2】



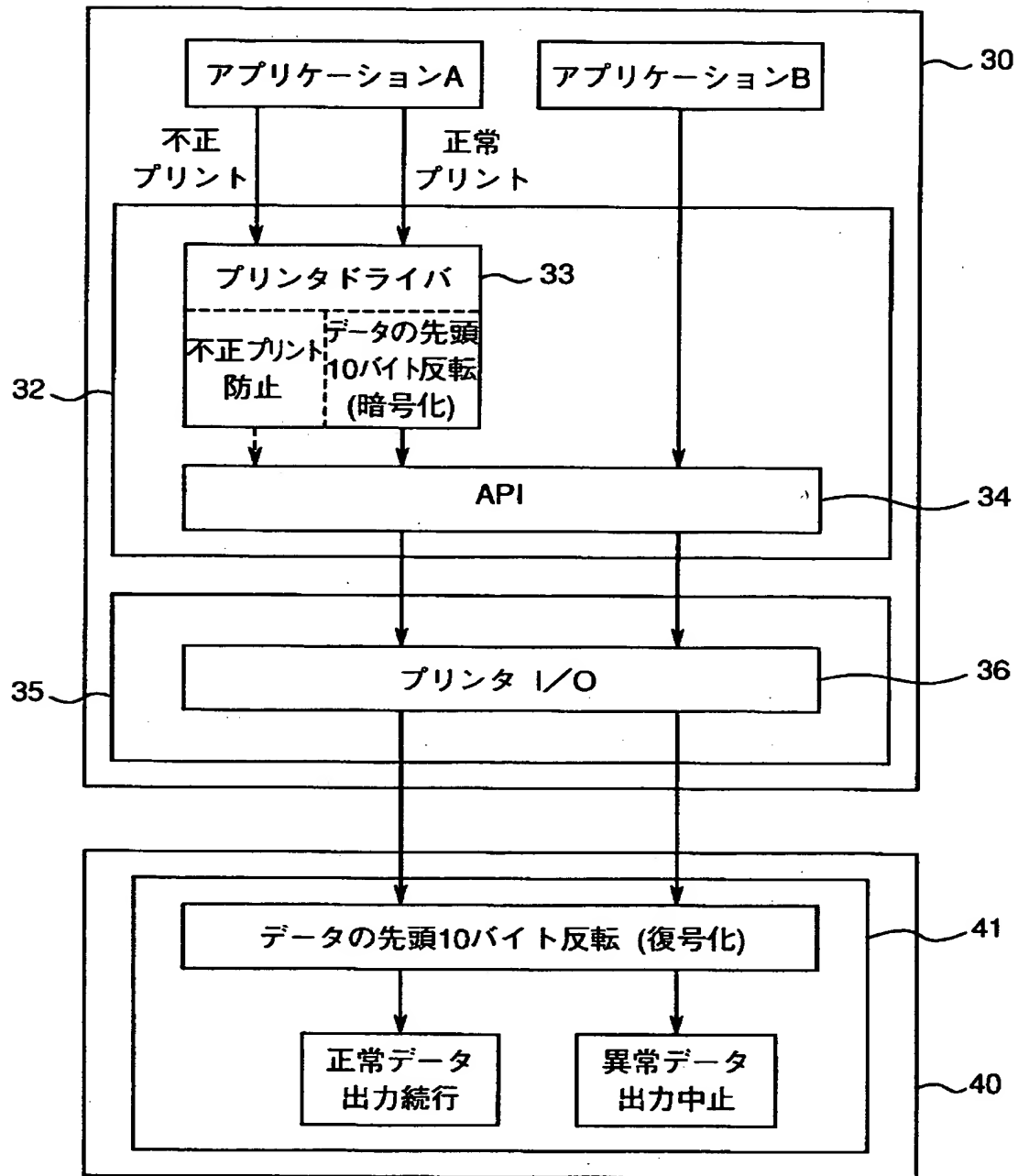
【図 3】



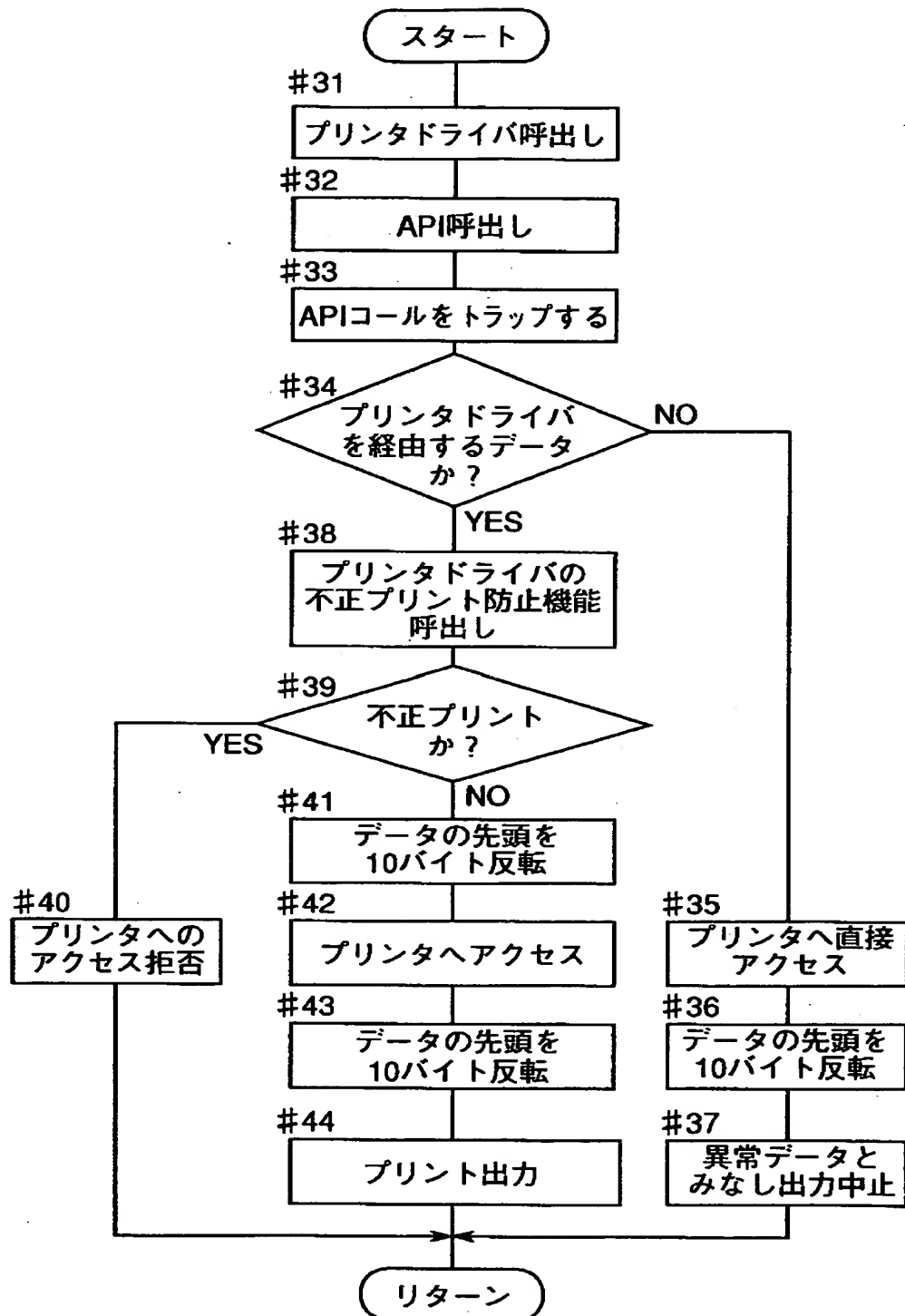
【図 4】



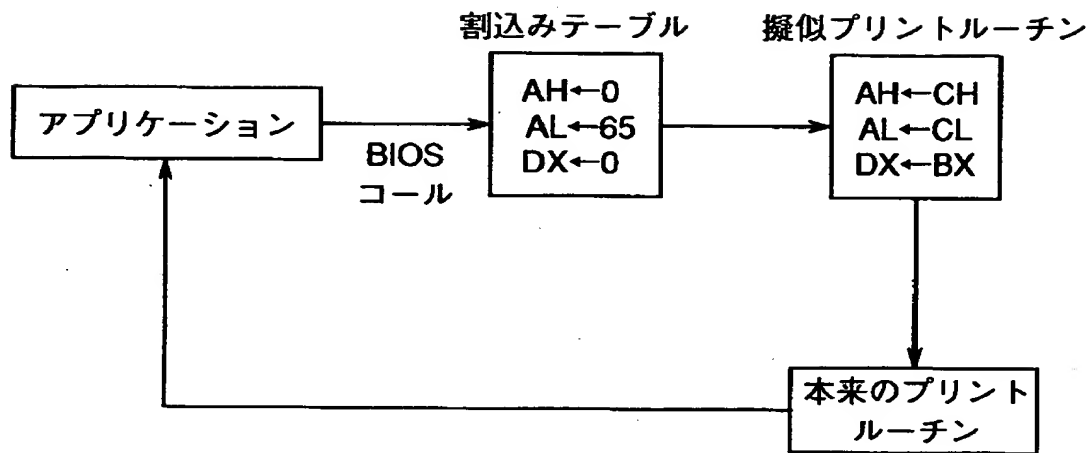
【図5】



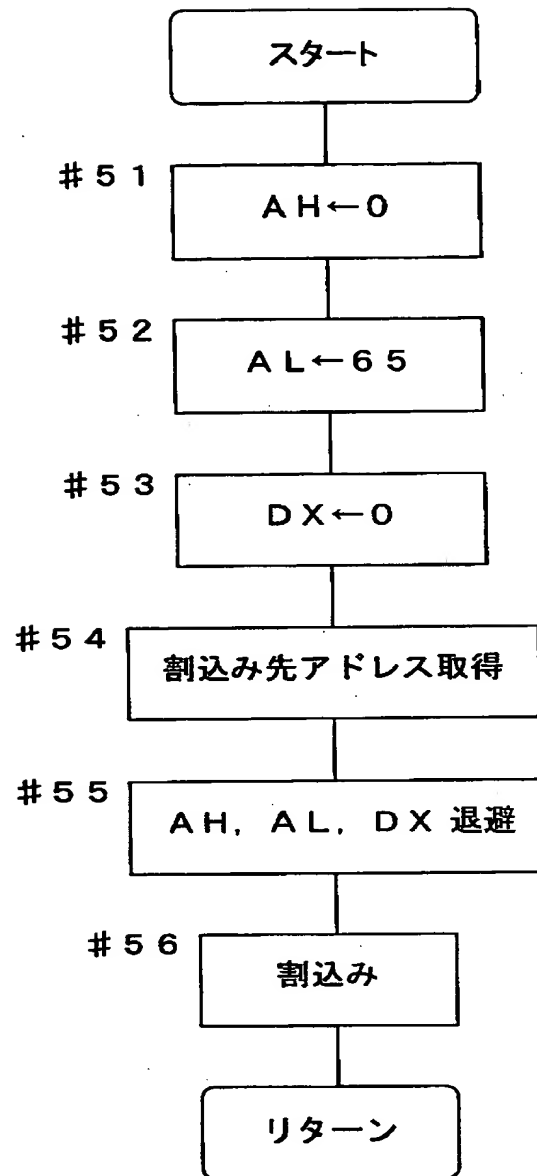
【図6】



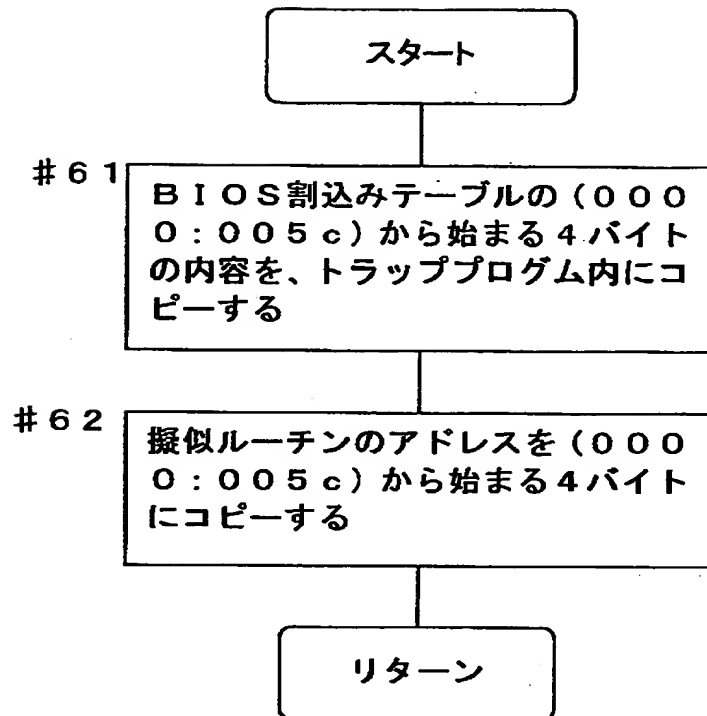
【図 7】



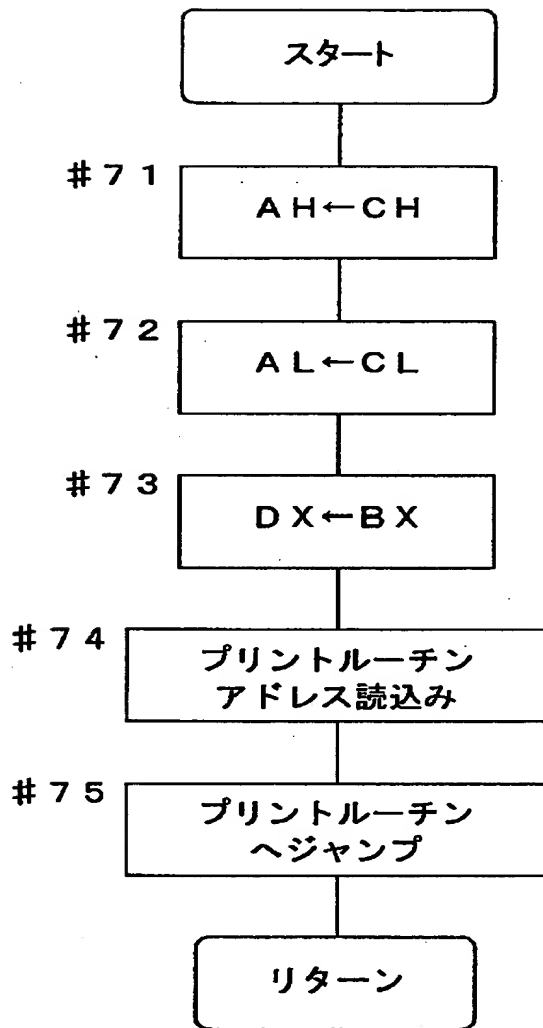
【図 8】



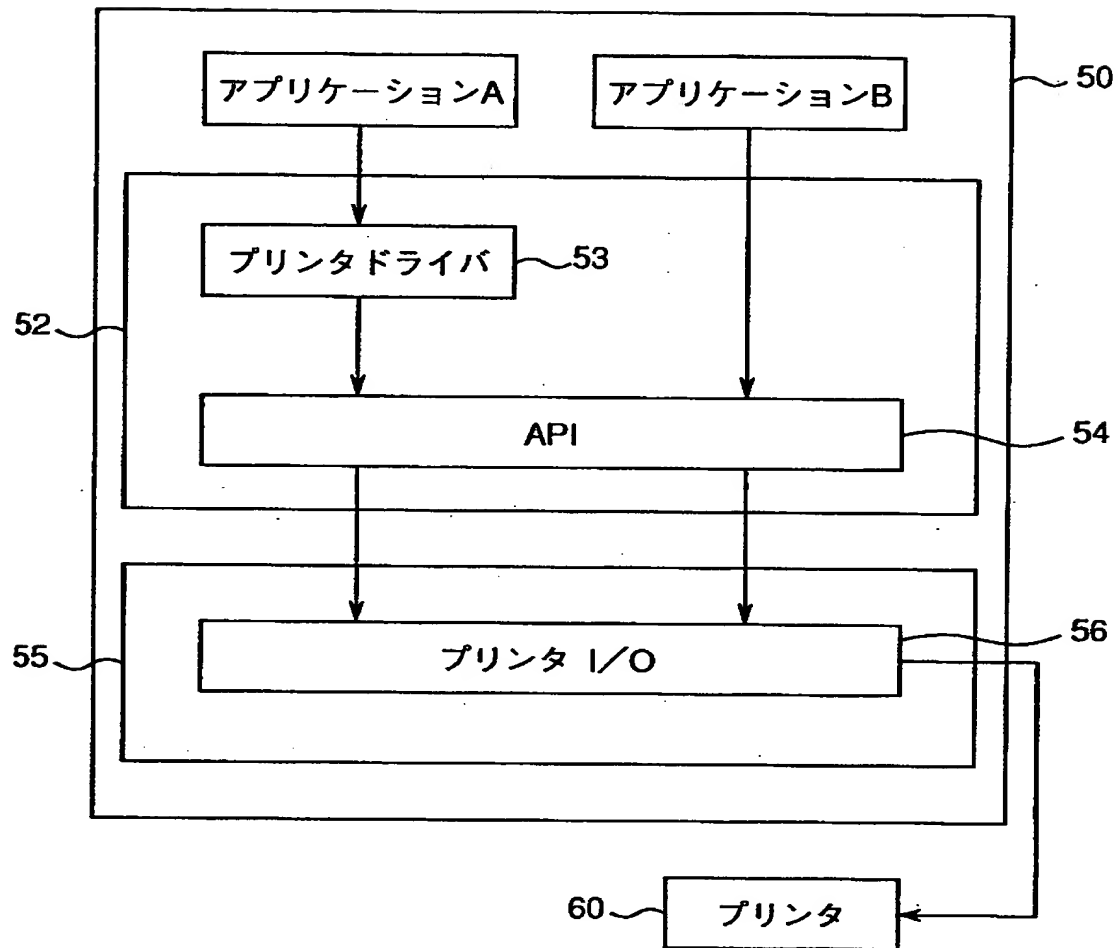
【図 9】



【図10】



【図 1 1】



【書類名】 要約書

【要約】

【課題】 安価且つ安全な出力システム及びそれに用いる出力方法並びに出力システムにおいて実行されるプログラムを記録した記録媒体を提供する。

【解決手段】 データ処理装置と該データ処理装置から送信されてきたデータを所定の形式で出力する出力装置とを備えた出力システムにおいて、上記データ処理装置に、上記出力装置を制御し得るドライバソフトウェアが組み込まれており、上記データ処理装置から出力装置へのデータ送信に際し、上記ドライバソフトウェアを経由する出力要求であるか否かを判断した上で、上記ドライバソフトウェアを迂回する出力要求に対して、上記出力装置へのデータ送信を禁止する。

【選択図】 図3

出 願 人 履 歴 情 報

識別番号 [000006079]

1. 変更年月日	1994年 7月20日
[変更理由]	名称変更
住 所	大阪府大阪市中央区安土町二丁目3番13号 大阪国際ビル
氏 名	ミノルタ株式会社